


<p>California Department of Justice CALIFORNIA JUSTICE INFORMATION SERVICES DIVISION Joe Dominic, Chief</p> 	<p>INFORMATION BULLETIN</p>	
<p><i>Subject:</i></p> <p>Purpose, Use, and Security of Criminal Offender Record Information (CORI)</p>	<p><i>No.</i> 19-04-CJIS</p> <p><i>Date:</i> 05-30-19</p>	<p><i>Contact for information:</i></p> <p>AuthorizationQuestions@doj.ca.gov</p>

TO: ALL APPLICANT AGENCIES

The purpose of this Information Bulletin is to explain important legal restrictions on the use, sharing, and maintenance of CORI for all agencies receiving CORI from the California Department of Justice (DOJ). **Please review this advisory carefully to understand your legal responsibilities with respect to the confidential information you are receiving.**

Definition of CORI

CORI means records and data compiled by criminal justice agencies for purposes of identifying criminal offenders. For each offender, CORI may include a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, and information pertaining to sentencing, incarceration, rehabilitation, and release. Criminal justice agencies throughout the state provide this information to the DOJ, which in turn is required to maintain it in a statewide repository.¹

Limited Access to CORI

The DOJ is required to provide CORI to specified agencies/entities to assist them in fulfilling their employment, licensing, and certification responsibilities. **CORI is privileged and confidential, and may not be disclosed except as specifically authorized by law.**²

CORI is exempt from disclosure under the California Public Records Act.

Agency access to CORI is restricted to its custodian of records and/or hiring authority charged with determining the suitability for employment, licensing, or certification of an applicant. The custodian of records is the individual designated by an agency as responsible for the security, storage, dissemination, and destruction of CORI furnished to the agency, and serves as the primary contact for the DOJ.³ The DOJ *must be notified* when the designated custodian of records no longer serves in that capacity for the agency/entity.⁴

¹ See Penal Code §§ 11075, 11105, 13102.

² See, e.g., Penal Code §§ 11075, 11076, 11081, 11105, and 11141 et seq; Civil Code §§ 1798, et seq.; Cal. Const., art. I, § 1.

³ Penal Code § 11102.2.

⁴ Penal Code § 11102.2, subdivision (h).

Dissemination/Use of CORI

CORI may only be used for official purposes, and only for the specific **purpose for which it was requested and provided**.

CORI may only be disclosed as specifically authorized by law. It may not be reproduced for secondary dissemination, transferred to, or shared with any other employing, licensing, or regulatory entity, or in response to a Public Records Act request. Unauthorized access, disclosure and/or misuse of CORI is a criminal offense.⁵

Data Security

CORI must be stored in a secure and confidential place, e.g., a locked area, room, file cabinet, or other storage container, with both physical and personnel security controls necessary to prevent unauthorized access and viewing. CORI kept in electronic format must be protected at the same level as physical media. Agency data-security responsibilities also include visitor control and physical access to workspaces, etc.⁶

Adequate Destruction Required

If the purpose for CORI access no longer applies, the agency must notify the DOJ as soon as possible that it is no longer interested in receiving subsequent arrest and disposition notifications, and, consistent with regulations, destroy any CORI in such a manner that the identity of the subject can no longer be ascertained.⁷ Secure disposal or destruction of physical media, including shredding or incineration, minimizes the risk of unauthorized access or use of CORI.

All agencies and organizations must ensure the disposal or destruction is witnessed or carried out by authorized personnel. If hard copy document maintenance services, or other noncriminal justice administrative functions, are performed on behalf of the agency, the authorized agency/entity must ensure that the contractor does not have uncontrolled access to the CORI.

It is vital that all agencies receiving CORI, either electronically or on paper, adhere to the aforementioned policies, procedures, and legal obligations. It is the responsibility of each applicant agency to ensure staff are aware of their own responsibilities to ensure the security of CORI, no matter if that information is maintained electronically, written, or in any other format; and to protect it from unauthorized access or use.

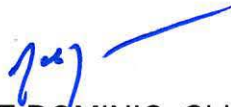
⁵ Penal Code §§ 11140 through 11144 (prescribing the penalties for misuse of criminal history record information); See also Government Code §§ 6200, 6201 (prescribing the penalties for the misuse of various government records, which include criminal history record information).

⁶ For more information regarding the information security requirements for CORI, please review and familiarize yourself with Appendix J—Noncriminal Justice Agency Supplemental Guidance, in the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy, available at <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center>.

⁷ Title 11, section 708 (a) of the California Code of Regulations.

Your assistance and cooperation are greatly appreciated. If you have any questions regarding these instructions, please contact the DOJ at AuthorizationQuestions@doj.ca.gov.

Sincerely,



JOE DOMINIC, Chief
California Justice Information Services Division

For XAVIER BECERRA
Attorney General